

1 Thomas R. Hogan, Esq., California State Bar No. 042048  
2 Phillip E. Maroc, Esq., California State Bar No. 188525  
3 LAW OFFICES OF THOMAS R. HOGAN  
4 60 South Market Street, Suite 1125  
5 San Jose, CA 95113-2332  
6 Telephone: (408) 292-7600

7 Attorneys for Defendant  
8 PUBLIC KEY PARTNERS

9  
10 UNITED STATES DISTRICT COURT  
11 FOR THE NORTHERN DISTRICT OF CALIFORNIA

12 ROGER SCHLAFLY,

13 Plaintiff,

14 v.

15 PUBLIC KEY PARTNERS and  
16 RSA DATA SECURITY, INC.,

17 Defendants.

No. CV 94 20512 SW (SW)

DECLARATION OF WILLIAM HUGH  
MURRAY IN SUPPORT OF  
DEFENDANT PUBLIC KEY PARTNERS  
MOTION FOR PARTIAL SUMMARY  
JUDGMENT

Date: August 27, 1997

Time: 10:00 a.m.

Dept: Ctrm. 4, 5th Floor

Judge: Hon. Spencer Williams

18 I, William Hugh Murray, declare:

19 1. I am a consultant, management trainer, and industry expert specializing in information  
20 systems security. I have more than forty years experience in information technology and more than  
21 twenty-five in information security. I am a Certified Information Systems Security Professional  
(CISSP). I have attached hereto, as Exhibit A, a copy of my curriculum vitae, which details my  
22 professional background. If called upon to testify, I would and could testify competently thereto.

23 2. This case concerns the business of application of cryptography to information security.  
24 Cryptography is the use of reversible logical and mathematical functions or algorithms to hide  
25 information from the unintended and to demonstrate its original and integrity.

26 3. Cryptography is a *logical* alternative to *physical* encapsulation or access control as a  
27 means of protecting information from disclosure or (undetected) alteration. Its historical advantage  
28 has been that it worked in such hostile applications and environments as radio communications.

FILED  
JUL 23 1997  
RICHARD W. WILKINS  
CLERK, U.S. DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE

265

1 Coupled with the modern computer, its advantage is that it is often cheaper than physical means.

2 4. Cryptography and physical encapsulation are both required for the protection of data;  
3 they complement each other. Both are necessary; neither is sufficient.

4 5. In modern cryptography the functions or algorithms are public but tailored to a  
5 specific use by a secret number called a "key". The two forms of key are *symmetric* and *asymmetric*.  
6 In conventional or symmetric key cryptography the same number is used to control the operation of  
7 the algorithm at both ends of the communication. Asymmetric key cryptography is the use of two  
8 different, but mathematically related numbers, at each end.

9 6. While the fundamental idea of cryptography is centuries old, until recently its use has  
10 been limited to state and military applications by its cost and difficulty of use. The commercial  
11 application of cryptography began in the banking industry in the late 1970's and accelerated with the  
12 adoption of the Data Encryption Standard by the National Bureau of Standards in 1977. It began in  
13 automated teller machines and spread slowly to electronic funds transfer applications. The primary  
14 suppliers to this market were IBM, NCR, Motorola, Diebold, Atalla and Racal.

15 7. The requirement for the private and commercial use of this technology is driven by the  
16 dramatic increase in data communications in open and shared networks. The effective, efficient, and  
17 widespread use of this technology is enabled by the decrease in cost and scale of the modern digital  
18 computer.

19 8. Asymmetric or public key cryptography was invented by Whitfield Diffie and Martin  
20 Hellman in 1977. While originally seen as an alternative to symmetric key cryptography, its success is  
21 an a complement to it. Asymmetric key cryptography is the single most novel invention in the history  
22 of cryptography. Asymmetric key cryptography's advantage is in large open populations of  
23 communicating parties. In such populations it tends to reduce the size of key tables and the amount  
24 of pre-arrangement.

25 9. The first practical implementation of asymmetric key cryptography was invented by  
26 Ronald Rivest, Adi Shamir, and Leonard Adelman. The acronym formed from their names, RSA, has  
27 become synonymous with the idea of public key cryptography. It includes the idea of a "digital  
28 signature," the ability not only to know that a message originated with a particular party and has not

1 been modified by the additional ability to demonstrate that, after the fact, to a third party.

2 10. Asymmetric key cryptography did not begin to appear in commercial products until  
3 the early 1990's where it is used primarily in hybrid products for the management of keys in  
4 symmetric key systems. Asymmetric key cryptography is only one of many alternative and  
5 competitive ways to accomplish such key management.

6 11. The eventual acceptance and application of public key cryptography was due to the  
7 vision and leadership of RSA Data Security, Inc, the corporation formed to exploit the patents  
8 granted to Rivest, Shamir and Adelman and assigned by them to MIT.

9 12. One inhibitor to the use of public key cryptography as an alternative to the more  
10 widely used and understood information security technology was the confusion, inconvenience and  
11 cost caused by overlapping patents.

12 13. RSA Data Security, Inc. and the owners of other public key patents formed Public  
13 Key Partners (PKP) to promote the use of asymmetric key technology as a more attractive alternative  
14 to other information.

15 14. While asymmetric key cryptography is currently enjoying competitive success and  
16 appears in many products, it represents a small part of the security content of those products.

17 15. Public Key Partners has been successful in licensing its patents. Its competitors  
18 include IBM, Northern Telecom, and Motorola.

19 16. Both the information security market and the cryptography sub-market are both  
20 diverse and competitive. There is no dominant technology, product or vendor.

21 I declare under the penalty of perjury that the foregoing is true and correct. Executed this  
22 23rd day of July, 1997, in San Jose, California.

23

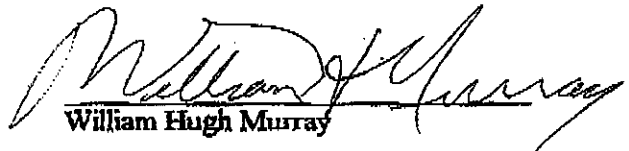
24 Dated: July 23, 1997

25

26

27

28

  
William Hugh Murray

A

### William Hugh Murray

Bill Murray is a consultant, management trainer, and industry expert specializing in information system security. He is a consultant to Deloitte & Touche's Information Protection Consulting Program. He has more than forty years experience in information technology and more than twenty-five in information security. He is a Certified Information System Security Professional (CISSP).

During twenty five years with IBM Mr. Murray held a number of management positions in application development, market support, and product development. As manager of Data Security Support Programs for a marketing division, he was responsible for articulating advice and counsel to IBM customers. As program manager of data security for a product group, he was responsible for developing the product security strategy.

In one IBM assignment Mr. Murray managed the development of the security subsystem for IBM's *Advanced Administrative System*. After two decades of operation this list-based access control system is still a model for many more modern systems.

He is a frequent contributor to the literature of edp audit, control and security. He is the author of the IBM publication, *Information System Security Controls and Procedures*. His articles have appeared in *Asset Protection* magazine, *EDP Audit Control and Security*, (IEEE) *Spectrum*, *Computers and Security*, *The Computer Security Journal*, *The IBM Systems Journal*, *Financial Executive Magazine*, and *Chief Financial Officer USA*. He serves on the editorial boards of major journals in the field, including *Computers and Security*, and His column appears regularly in *Info Security News*.

He served as vice-chairman of the U. S. Small Business Administration Computer Security and Education Advisory Council. He chaired the ISSA committee to define the common body of knowledge (CBOK). He is on the board of directors of the International Information System Security Certification Consortium (ISC\*\*2) and is chairman of its advisory committee.


He is a popular speaker on a wide range of security, audit and control topics. National programs on which he has appeared include the AICPA, the IIA, the EDP Auditors Association, the Information System Security Association, the National Computer Security Conference, the National Crime Prevention Institute, SHARE and GUIDE. He has appeared before COMPACS, COMPSEC, SEAS, GUIDE, and the Diebold Research Program in Europe, and the Australia-New Zealand Association for the Advancement of Science. He was chosen to chair the 13th, 16th, 17th and 20th annual Computer Security Institute conferences.

In 1987 he received the *Fitzgerald Memorial Award* for leadership in data security. In 1989 he received the *Joseph J. Wasserman Award* for contributions to security, audit, and control. In 1995 he received the Computer Security Institute's Lifetime Achievement Award.

**WILLIAM MURRAY (CONTINUED)**

He is a director of Telequip Corporation.

Mr. Murray holds the Bachelor of Science degree in Business Administration from Louisiana State University, and is a graduate of the Jesuit Preparatory High School of New Orleans.

**WILLIAM MURRAY (CONTINUED)****WILLIAM HUGH MURRAY***Executive Consultant***Information System Security**  


Mr. Murray is a leading expert in the area of information protection.

**EXPERIENCE**

Mr. Murray is a consultant, management trainer, and industry expert in information system security. He has more than forty years of experience in information technology and more than twenty-five years experience in information protection.

- ☐ During twenty-five years with IBM, he held a number of management positions in application development, market support, and product development. As manager of Data Security Support Programs for a marketing division, he was responsible for market support for the **Resource Access Control Facility** for IBM's VM and MVS operating systems. As program manager of data security for the Communications Product Group, he was responsible for authoring the product security strategy. He was one of the early participants in the definition of security requirements for IBM's System Application Architecture including the common user and common cryptographic architectures.
- ☐ In one IBM assignment, he managed the development of the security subsystem for IBM's Advanced Administrative System. After almost two decades of operation, this list-based access control system is still a model for many more modern systems.
- ☐ During three years with another consulting firm, Mr. Murray was responsible for research, methodology development, client service and marketing.
- ☐ He is the author of the IBM publication, **Information System Security Controls and Procedures**. Now in its fourth printing, this may be the most widely cited publication in the field.

**WILLIAM MURRAY (CONTINUED)**

- ☐ He is the author of the **IBM Security Assessment Questionnaire**. The "Orange Card" is the most widely used security self-assessment in the world.
- ☐ He is the author of the security architecture chapter and the LAN security chapter for the **Handbook of Information Security Management**. He is the author of the chapter on DOS in the **Computer Security Reference Book**. His chapter on Security, Audit, and Control of Client-Server Architecture will appear in a forthcoming book to be published by Auerbach.
- ☐ His column, *Alerts and Alarms*, appears regularly in **Info Security News**.
- ☐ Recent engagements include design of the security for a cash management application for a money center bank; security reviews for internet banking applications for two large banks; e-commerce policy for a property and casualty insurance company, enterprise security architecture for a life insurance company; review of security for internet banking for a private bank; selection of cryptographic products for worldwide private banking network. He also consults to a number of information security technology companies.

**PROFESSIONAL**

He is a regular contributor to the literature of EDP audit, control and security. He is the author of the IBM publication *Data Security Controls and Procedures*. His articles have appeared in *Asset Protection* magazine, *EDP Audit Control and Security*, *Computers and Security*, *The Computer Security Journal*, *The IBM Systems Journal*, *The Communications of the ACM*, *Financial Executive Magazine*, and *Chief Financial Officer USA*.

Mr. Murray is a popular speaker on a wide range of data security topics. National programs on which he has appeared include the National Computer Security conference, AICPA, the IIA, the EDP Auditors Association, The National Crime Prevention Institute, SHARE, and GUIDE. He has appeared before SEAS, GUIDE, and the Diebold Research Program in Europe, and the Australia-New Zealand Association for the Advancement of Science.



**WILLIAM MURRAY (CONTINUED)**

Chairman of the 13th, 16th, 17th and 20th Annual Computer Security Institute Conferences.

Chairman of the ISSA's Common Body of Knowledge Committee and is a member of the Future Technology Committee of the National Institute of Standards and Technology's Telecommunications and Communications Security Council.

1987 Fitzgerald Memorial Award for leadership in data security.

1989 Joseph J. Wasserman Award for contributions to security, audit and control

1995 Computer Security Institute Lifetime Achievement Award

**BUSINESS**

Director, Telequip Corporation

**CERTIFICATION**

Certified Information System Security Professional